What is claimed is:

1. A method by which a terminal (10) determines whether a candidate RAND included in a RAND challenge is a member of a set of previously used RANDs, characterized by:

a step (31) of encoding the previously used RANDs using a data structure (21) consisting of an ordered set of components having component values derived from the previously used RANDs wherein each component has a value of one or zero depending on whether it is pointed to by one or more pointers each having a value based on a digest of all the bits of a respective previously used RAND or having a value otherwise derived from all the components of a respective previously used RAND so that in either case all bits of the RAND contribute in determining the value of the component; and

a step (32) of checking the data structure (21) to determine whether the data structure indicates whether the candidate RAND is a member of a set of previously used RANDs;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate RAND is not an element of the set of previously used RANDs.

2. A method as in claim 1, wherein in the step (31) of encoding the previously used RANDs, a set of hash functions is used each having a range equal to the number of components of the data structure (21), and for each previously used RAND, each of the hash functions is evaluated and the component in the ordered set of components at the position indicated by the hash function value is set to one.

3. A method as in claim 2, wherein the previously used RAND values serve as the hash functions based on using the RAND values as pointers to components of the data structure (21).

4. A method as in claim 1, wherein the data structure (21) is a multi-part data structure (21) with each part having an upper limit on the number of RAND values it can indicate as belonging to the set of previously used RAND values, and further wherein when an upper limit is reached for one of the parts, another of the parts is reset.

5. A computer program product comprising: a computer readable storage structure embodying computer program code thereon for execution by a computer processor in a terminal (10), with said computer program code characterized in that it includes instructions for performing the steps of the method of claim 1.

6. An apparatus included in a telecommunication terminal (10) and by which the telecommunication terminal (10) determines whether a candidate RAND included in a RAND challenge is a member of a set of previously used RANDs, characterized by:

means (11 12 31) for encoding the previously used RANDs using a data structure (21) consisting of an ordered set of components having component values derived from the previously used RANDs wherein each component has a value of one or zero depending on whether it is pointed to by one or more pointers each having a value based on a digest of all the bits of a respective previously used RAND or having a value otherwise derived from all the components of a respective previously used RAND so that in either case all bits of the RAND contribute in determining the value of the component; and

means (11 12 32) for checking the data structure (21) to determine whether the data structure indicates whether the candidate RAND is a member of a set of previously used RANDs;

wherein the data structure (21) is such as to at least provide a true answer as to whether the candidate RAND is not an element of the set of previously used RANDs.

7. A system, comprising a telecommunication terminal (10) and a radio access network configured for cellular communication with the telecommunication terminal (10), characterized in that the telecommunication terminal (10) includes an apparatus as in claim 6.